Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **MAR 2008**	2. REPORT TYPE	3. DATES COVERED **00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE
Trust in Integrated Circuits

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Defense Advanced Research Projects Agency,Microsystems Technology Office,Arlington,VA,22203-1714

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM202438. Presesnted at GOMACTech-08, Microsensor Technologies: Enabling Information on Demand, 17-20 Mar 2008, Las Vegas, NV

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**3**	

GOMACTech08

To: All GOMACTech Participants

From: Gerry Borsuk, Conference Chair

Subject: GOMACTech 2008 Proceedings -- Distribution Clarification

Date: June 1th, 2008

1. Distribution Statements are used in marking technical data to denote the extent of its availability for secondary distribution, release, and disclosure without additional approvals or authorizations by the originator or controlling office. (DoDD 5230.24)

2. Be advised that the GOMACTech 2008 Proceedings CD-ROM as a compilation is Distribution X.

3. All unmarked component papers are to be controlled and handled in accordance with Distribution X.

3. The markings on the following two papers are changed to Distribution X:

> Title: "Family of UGS Demonstration" by Army Research Laboratory (ARL)
> Distribution C is changed to Distribution X
>
> Title: "Defining MAC1 Components Through a Top Down Approach" from SAIC
> FOUO is changed to Distribution X

4. Only those papers marked "Approved for Public Release" have no distribution constraints.

5. Please keep this letter with your copy of the GOMACTech 2008 Proceedings on CD-ROM.

G W Borsuk

Gerry Borsuk, GOMACTech 2008 Conference Chair

Trust in Integrated Circuits*

Dr. Dean R. Collins
Deputy Director
Microsystems Technology Office
Defense Advanced Research Projects Agency
Arlington, Virginia, 22203-1714
+1-571-218-4650 • dean.collins@darpa.mil

DARPA's TRUST in Integrated Circuits program is directed at ensuring trust in integrated circuits that are designed and fabricated under untrusted conditions. This issue has been identified in a recent Defense Science Board study [1] and the problems described in the study are becoming more acute. The majority of Integrated Circuits (ICs) used in complex modern military systems are made off-shore. Field Programmable Gate Arrays (FPGA's) are the dominate IC used in modern weapons systems and the vast majority of FPGA's are made off shore. At the present time the US does not have a comprehensive program to certify that the ICs that are going into U.S. weapons systems do not contain malicious circuits. This paper focuses on describing the structure and goals of the program, along with the challenges facing the effort. The program has wide participation with numerous US government departments. A brief description will be given of some of the novel approaches initially being deployed to address the challenges.

The TRUST program is presently focused on three Tasks for ensuring trust in integrated circuits:

1. Ensuring trust in the design cycle for Application Specific Integrated Circuits (ASIC's).
2. Ensuring trust when an ASIC is fabricated in an untrusted foundry
3. Ensuring trust when employing FPGA's in military systems.

The program structure is composed of three government teams and four prime contractors:

a. Government Red Team (MIT Lincoln Labs lead)

b. Government Test Article Team (USC/ISI)

c. Government Metrics Team (JHU/APL)

d. System Integrator (Raytheon)

e. Hardware and Software – Tasks 1, 2&3 (Raytheon, BAE Systems, Analytic Solutions Inc., R3 Logic, and Cadence)

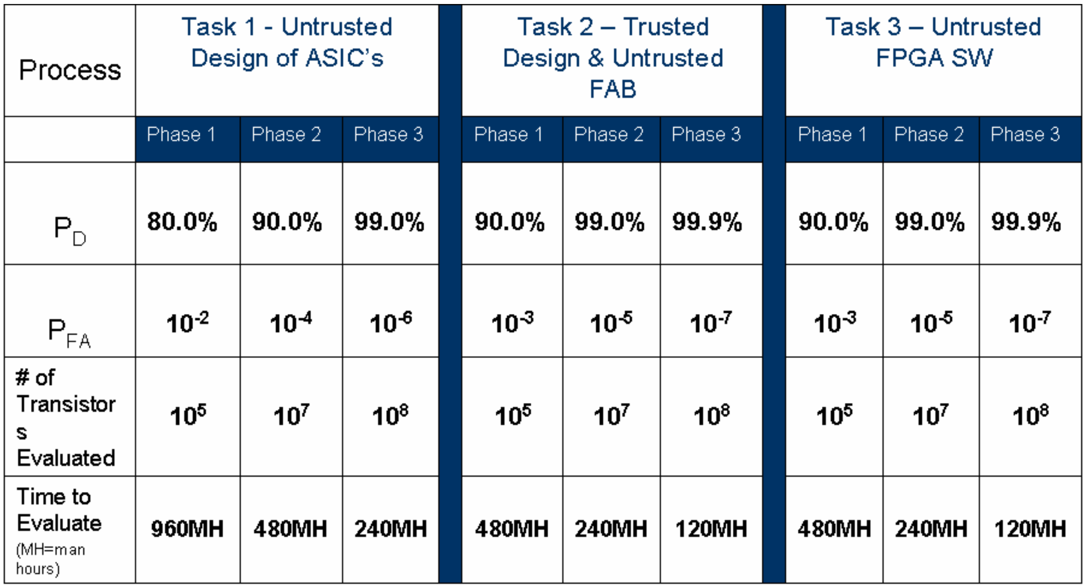
f. FPGA's - Task 3 (Luna)

g. X-ray Analysis - Task 2 (USC/Information Sciences Institute, Xradia, Stanford & Argonne National Lab.)

The goals of the program for each for the three tasks are shown in Figure 1. The program consists of three one year phases. The metrics for the program become more difficult in each of the subsequent phases with the number of transistors examined increasing and the time allowed to perform the examination decreasing. At the same time the required probability of detection of a change to the integrated circuit increases and the probability of declaring a good circuit as bad decreases. The TRUST program employs a unique approach to quantifying TRUST in terms of P_d/P_{fa}, in contrast to previous attack/defense tree methods, and also focuses on changes rather than Trojan circuits. The Test Article Team is producing a series of ICs and software to provide a uniform set of test articles for all performers

The challenges for the program are significant for each of the tasks. Task 1, the design task, is perhaps the challenging; it has been called the if-and–only-if (iff) problem. Present set of commercial design tools focus on making sure the IC meets all the required functionality defined in the specification. In general the tools do not focus on determining if additional functionality has been added into the circuit design which was contained in the original specification. These design tools are proprietary, complex, contain many million lines of code, may be written outside the US, are in constant version changes, and may require the tools to "call home" for part of their functionality. However one can compare the results by using tools from different vendors to see if there are significant differences. The case of using 3rd Party Intellectual Property (IP) in the design process presents additional concern since these codes are written by vendors from many parts of the world, are highly proprietary, and in many cases contain "unused" functions.

[*] Approved for Public Release, distribution unlimited



Process	Task 1 - Untrusted Design of ASIC's			Task 2 – Trusted Design & Untrusted FAB			Task 3 – Untrusted FPGA SW		
	Phase 1	Phase 2	Phase 3	Phase 1	Phase 2	Phase 3	Phase 1	Phase 2	Phase 3
P_D	80.0%	90.0%	99.0%	90.0%	99.0%	99.9%	90.0%	99.0%	99.9%
P_{FA}	10^{-2}	10^{-4}	10^{-6}	10^{-3}	10^{-5}	10^{-7}	10^{-3}	10^{-5}	10^{-7}
# of Transistors Evaluated	10^5	10^7	10^8	10^5	10^7	10^8	10^5	10^7	10^8
Time to Evaluate (MH=man hours)	960MH	480MH	240MH	480MH	240MH	120MH	480MH	240MH	120MH

Figure 1: TRUST Go/No-go metrics

Task 2, the foreign foundry related task, is basically a combined destructive and non-destructive reverse engineering task. The primary challenges for this task are time to perform the destructive reverse engineering and the ability to make effective non-destructive measurements. However the sheer magnitude of the reverse engineering tasks will require many innovations to comprehend: small feature detection (90 nm and below nodes), large number of transistors, multiple layers in each device (9 or more), more complex materials, the requirement that delayering be done on only one device, and the tremendous computational effort required to compare the information derived from the delayered device to the original GDS II design.

Task 3, the FPGA related task, is very important since FPGA's are becoming the IC of choice for both commercial and military systems. Domestic based companies dominate the FPGA market, however almost all FPGA's are fabricated offshore. The design process suffers from the same design vulnerabilities as ASIC's including the use of offshore 3rd party IP. However the design flow for FPGA's presents additional verification issues. The design process for FPGA's starts out using many same vendor design tools used for ASIC's, however at a certain point the design flow enters into tools which are highly proprietary and FPGA vendor specific. Presently there is no vendor independent method of verifying the bitstream loaded into a FPGA. FPGA's are by definition field programmable and commercially available. Hence the possibility of substitution or reprogramming in the field can occur. Finally, FPGA's may contain vendor specific "private" functions which are not revealed to the general user, and which could be used for unintended purposes. The challenges for Task 3 include:

a. A vendor independent method of verifying that the bit stream contains the functionality specified and nothing more and nothing less.
b. A vendor independent method to verify the correct loading of the bitstream into the FPGA.
c. A vendor independent method to ensure that a proper bitstream loaded into a FPGA is not modified at a later time by means either external or internal to the FPGA.
d. A vendor independent method to uniquely identify a specific FPGA.

The TRUST program presently contains many novel techniques and approaches to measure trust. These include X-ray Tomography, simultaneous Focused Ion Beam etching and Scanning Electron Microscope imaging, Boolean Equivalence Checking, Physically Uncloneable Functions, electromagnetic probes, GDS II to netlist generation and advanced pattern recognition. Even with these advanced tools the program goals remain extremely challenging.

Reference [1] http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf